Practitioner's Docket No. NAI1P492/03.028.01 *PATENT*

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Colin John Blamires et al.

Application No.: 10/620,364 Group No.: 2134
Filed: 07/17/2003 Examiner: Simitoski, Michael J.
For: MALWARE SCANNING USING A BOOT WITH A NON-INSTALLED OPERATING SYSTEM AND DOWNLOAD OF MALWARE DETECTION FILES

Mail Stop Appeal Briefs – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF
(PATENT APPLICATION--37 C.F.R. § 41.37)

1. This brief is in furtherance of the Notice of Appeal, filed in this case on 09/17/2007, and in response to the Notice of Panel Decision from Pre-Appeal Brief Review, mailed 11/14/2007.

2. STATUS OF APPLICANT

   This application is on behalf of other than a small entity.

3. FEE FOR FILING APPEAL BRIEF

   Pursuant to 37 C.F.R. § 41.20(b)(2), the fee for filing the Appeal Brief is:

other than a small entity	$510.00
Appeal Brief fee due	**$510.00**

4. EXTENSION OF TERM

   The proceedings herein are for a patent application and the provisions of 37 C.F.R. § 1.136 apply.

   Applicant believes that no extension of term is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

5. TOTAL FEE DUE

   The total fee due is:

Appeal brief fee	$510.00
Extension fee (if any)	$0.00
TOTAL FEE DUE	**$510.00**

6. FEE PAYMENT

Authorization is hereby made to charge the amount of $510.00 to Deposit Account No. 50-1351 (Order No. NAI1P492).

7. FEE DEFICIENCY

If any additional extension and/or fee is required, and if any additional fee for claims is required, charge Deposit Account No. 50-1351 (Order No. NAI1P492).

Date: December 13, 2007

/KEVINZILKA/
Signature of Practitioner

Reg. No.: 41,429
Tel. No.: 408-971-2573
Customer No.: 28875

Kevin J. Zilka
Zilka-Kotab, PC
P.O. Box 721120
San Jose, CA 95172-1120

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	
Blamires et al.	Group Art Unit: 2134
Application No. 10/620,364	Examiner: Simitoski, Michael J.
Filed: 07/17/2003	Atty. Docket No. NAI1P492/03.028.01
For: MALWARE SCANNING USING A BOOT WITH A NON-INSTALLED OPERATING SYSTEM AND DOWNLOAD OF MALWARE DETECTION FILES	Date: 12/13/2007

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

ATTENTION: Board of Patent Appeals and Interferences

APPEAL BRIEF (37 C.F.R. § 41.37)

This brief is in furtherance of the Notice of Appeal, filed in this case on 09/17/2007, and in response to the Notice of Panel Decision from Pre-Appeal Brief Review, mailed 11/14/2007.

The fees required under § 1.17, and any required petition for extension of time for filing this brief and fees therefor, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief contains these items under the following headings, and in the order set forth below (37 C.F.R. § 41.37(c)(i)):

I REAL PARTY IN INTEREST
II RELATED APPEALS AND INTERFERENCES
III STATUS OF CLAIMS
IV STATUS OF AMENDMENTS
V SUMMARY OF CLAIMED SUBJECT MATTER

VI GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

VII ARGUMENT

VIII CLAIMS APPENDIX

IX EVIDENCE APPENDIX

X RELATED PROCEEDING APPENDIX

The final page of this brief bears the practitioner's signature.

I REAL PARTY IN INTEREST (37 C.F.R. § 41.37(c)(1)(i))

The real party in interest in this appeal is McAfee, Inc.

II RELATED APPEALS AND INTERFERENCES (37 C.F.R. § 41.37(c) (1)(ii))

With respect to other prior or pending appeals, interferences, or related judicial proceedings that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no other such appeals, interferences, or related judicial proceedings.

A Related Proceedings Appendix is appended hereto.

III STATUS OF CLAIMS (37 C.F.R. § 41.37(c) (1)(iii))

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1-3, 7-11, 15-19 and 23-31

B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims withdrawn from consideration: None
2. Claims pending: 1-3, 7-11, 15-19 and 23-31
3. Claims allowed: None
4. Claims rejected: 1-3, 7-11, 15-19 and 23-31
5. Claims cancelled: 4-6, 12-14 and 20-22

C. CLAIMS ON APPEAL

The claims on appeal are: 1-3, 7-11, 15-19 and 23-31

See additional status information in the Appendix of Claims.

IV STATUS OF AMENDMENTS (37 C.F.R. § 41.37(c)(1)(iv))

As to the status of any amendment filed subsequent to final rejection, there are no such amendments after final.

V SUMMARY OF CLAIMED SUBJECT MATTER (37 C.F.R. § 41.37(c)(1)(v))

With respect to a summary of Claim 1, as shown in Figures 1-2 et al., a removable physical media bearing a computer program operable to control a computer to detect malware is provided. In use, said computer is booted with a non-installed operating system read from said removable physical media instead of an installed operating system stored on said computer (e.g. see item 16 of Figure 2, etc.). Additionally, network support code for said computer read from said removable physical media is loaded (e.g. see item 18 of Figure 2, etc.). Further, one or more malware detection files are downloaded from a remote computer (e.g. see item 24 of Figure 2, etc.). Still yet, malware detection is performed upon said computer using said one or more malware detection files (e.g. see item 26 of Figure 2, etc.). Moreover, a secure network connection to said remote computer is established (e.g. see item 22 of Figure 2, etc.). Also, a firewall computer (e.g. see item 4 of Figure 1, etc.) disposed between said computer (e.g. see item 2 of Figure 1, etc.) and said remote computer (e.g. see item 6 of Figure 1, etc.) is operable to block a connection between said computer and said remote computer other than said secure network connection. In addition, said network support code is used to enable said computer to establish said secure network connection via said firewall computer to said remote computer. See, for example, page 3, lines 16-27; page 4, lines 24-32; and page 7, lines 25-27 et al.

With respect to a summary of Claim 9, as shown in Figures 1-2 et al., a method of detecting malware upon a computer is provided. In use, said computer is booted with a non-installed operating system read from a removable physical media instead of an installed operating system stored on said computer (e.g. see item 16 of Figure 2, etc.). Additionally, network support code for said computer read from said removable physical media is loaded (e.g. see item 18 of Figure 2, etc.). Further, one or more malware detection files is downloaded from a remote computer (e.g. see item 24 of Figure 2, etc.). Still yet, malware detection is performed upon said computer using said one or more malware detection files (e.g. see item 26 of Figure 2, etc.). Also, a secure network connection to said remote computer is established (e.g. see item 22 of Figure 2, etc.). Moreover, a firewall (e.g. see item 4 of Figure 1, etc.) disposed between said computer (e.g. see item 2 of Figure 1, etc.) and said remote computer (e.g. see item 6 of Figure 1, etc.) is operable to block a connection between said computer and said remote computer other than said secure network connection. In addition, said network support code is used to enable said computer to

establish said secure network connection via said firewall to said remote computer. See, for example, page 3, lines 16-27; page 4, lines 24-32; and page 7, lines 25-27 et al.

With respect to a summary of Claim 17, as shown in Figures 1-2 et al., a computer operable to detect malware upon said computer is provided. In use, said computer is booted with a non-installed operating system read from a removable physical media instead of an installed operating system stored on said computer (e.g. see item 16 of Figure 2, etc.). Additionally, network support code for said computer read from said removable physical media is loaded (e.g. see item 18 of Figure 2, etc.). Further, one or more malware detection files are downloaded from a remote computer (e.g. see item 24 of Figure 2, etc.). Still yet, malware detection is performed upon said computer using said one or more malware detection files (e.g. see item 26 of Figure 2, etc.). Moreover, a secure network connection to said remote computer is established (e.g. see item 22 of Figure 2, etc.). Also, a firewall computer (e.g. see item 4 of Figure 1, etc.) disposed between said computer (e.g. see item 2 of Figure 1, etc.) and said remote computer (e.g. see item 6 of Figure 1, etc.) is operable to block a connection between said computer and said remote computer other than said secure network connection. In addition, said network support code is used to enable said computer to establish said secure network connection via said firewall computer to said remote computer. See, for example, page 3, lines 16-27; page 4, lines 24-32; and page 7, lines 25-27 et al.

With respect to a summary of Claim 25, as shown in Figures 1-2 et al., a server computer is provided which is connected by a network link to a computer detecting malware upon said computer, said server computer comprising a processor. In use, a secure network connection to said computer is established (e.g. see item 22 of Figure 2, etc.). Additionally, one or more malware detection files are loaded to said computer (e.g. see item 24 of Figure 2, etc.). Further, a firewall (e.g. see item 4 of Figure 1, etc.) disposed between said computer (e.g. see item 2 of Figure 1, etc.) and said server computer (e.g. see item 6 of Figure 1, etc.) is operable to block a connection between said computer and said server computer other than said secure network connection. Still yet, said computer is booted with a non-installed operating system read from a removable physical media instead of an installed operating system stored on said computer (e.g. see item 16 of Figure 2, etc.). Moreover, network support code is loaded for said computer read from said removable physical media (e.g. see item 18 of Figure 2, etc.). In addition, said

network support code is used to enable said computer to establish said secure network connection via said firewall to said server computer. Also, malware detection is performed upon said computer using said one or more malware detection files (e.g. see item 26 of Figure 2, etc.). See, for example, page 3, lines 16-27; page 4, lines 24-32; and page 7, lines 25-27 et al.

Of course, the above citations are merely examples of the above claim language and should not be construed as limiting in any manner.

VI GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL (37 C.F.R. § 41.37(c)(1)(vi))

Following, under each issue listed, is a concise statement setting forth the corresponding ground of rejection.

Issue # 1: The Examiner has rejected Claims 1-3, 7-11, 15-19, 23-25 and 28-30 under 35 U.S.C. 103(a) as being unpatentable over Reinert (U.S. Patent No. 6,347,375) in view of Yadav (U.S. Publication No. 2003/0149887), and in further view of Stallings ("Network Security Essentials, Applications and Standards").

Issue #2: The Examiner has rejected Claims 26-27 under 35 U.S.C. 103(a) as being unpatentable over Reinert (U.S. Patent No. 6,347,375) in view of Yadav (U.S. Publication No. 2003/0149887), in view of Stallings ("Network Security Essentials, Applications and Standards"), and in further view of Khatri (U.S. Patent No. 6,721,883).

Issue #3: The Examiner has rejected Claim 31 under 35 U.S.C. 103(a) as being unpatentable over Reinert (U.S. Patent No. 6,347,375) in view of Yadav (U.S. Publication No. 2003/0149887), in view of Stallings ("Network Security Essentials, Applications and Standards"), and in further view of McCoskey (U.S. Publication No. 2003/0028889).

Issue #4: The Examiner has not specifically rejected Claims 5, 9, 13, 17, 21, 25, and 31 under 35 U.S.C. 112. However, in the Office Action dated 05/15/2007, the Examiner has responded to appellant's arguments from the Amendment dated 03/12/2007 regarding the 35 U.S.C. 112 rejection from the Office Action dated 12/11/2006, in a manner that reaffirms such earlier rejection. Thus, for the purposes of this appeal, it is assumed that such rejection still stands.

VII ARGUMENT (37 C.F.R. § 41.37(c)(1)(vii))

The claims of the groups noted below do not stand or fall together. In the present section, appellant explains why the claims of each group are believed to be separately patentable.

Issue # 1:

The Examiner has rejected Claims 1-3, 7-11, 15-19, 23-25 and 28-30 under 35 U.S.C. 103(a) as being unpatentable over Reinert (U.S. Patent No. 6,347,375) in view of Yadav (U.S. Publication No. 2003/0149887), and in further view of Stallings ("Network Security Essentials, Applications and Standards").

Group #1: Claims 1-3, 7-11, 15-19, 23-25 and 28

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on appellant's disclosure. *In re Vaeck,* 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

With respect to the obviousness of combining the Reinert and Yadav references, the Examiner has argued that "it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Reinert [with Yadav] to connect to the remote computer via a secure connection." To the contrary, appellant respectfully asserts that it would not have been obvious to combine the teachings of the Reinert and Yadav references, especially in view of the vast evidence to the contrary.

Specifically, the Reinert reference teaches that "the present invention discloses a method and apparatus for providing up-to-date virus scanning of a local computer by a remote computer

comprising those situations where the normal operating system of the local computer is not operable" (Col. 3, lines 44-48 - emphasis added). On the other hand, the Yadav reference teaches "[n]etwork intrusion detection [that] accurately identifies and takes into consideration currently running network applications by examining machine instructions embodying those applications" (Abstract, lines 1-4 - emphasis added).

If the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims *prima facie* obvious. *In re Ratti*, 270 F.2d 810, 123 USPQ 349 (CCPA 1959)

Combining a method where the normal operating system is not operable, as in Reinert, with an intrusion detection system that takes into consideration currently running network applications, as in Yadav, would require an impermissible change in the principle of operation of Reinert, contrary to *In re Ratti*. Thus, the Examiner's proposed combination is inappropriate. To this end, the first element of the *prima facie* case of obviousness has not been met.

More importantly, appellant also respectfully asserts that the third element of the *prima facie* case of obviousness has not been met by the prior art excerpts relied on by the Examiner. For example, with respect to the independent claims, the Examiner has relied on Col. 7, lines 4-5 and lines 65-67 from Reinert; paragraphs 0042-0044 from Yadav; pages 320-323, and the "private network" in Fig. 10.1(a) from Stallings to make a prior art showing of appellant's claimed technique "wherein said network support code is used to enable said computer to establish said secure network connection via said firewall computer to said remote computer" (see this or similar, but not necessarily identical language in the independent claims).

Appellant respectfully asserts that the excerpts from Reinert relied upon by the Examiner merely teach that "[i]f any viruses are detected, the user may then connect to the remote computer utilizing the communications program" (Col. 7, lines 4-5), and that "[i]f the local user desires to connect with the remote computer 54, a communications program is invoked by the local user to establish a communications connection" (Col. 7, lines 65-67 – emphasis added). Additionally, the excerpts from Yadav merely teach that "the SOC 270 and the NIDS may communicate over a

virtual private network (VPN) 284, with its own encryption and security features, or use Secure Sockets Layer (SSL) to create a secure connection" (Paragraph 0044). Furthermore, the excerpts cited from Stallings only generally teach "FIREWALL DESIGN PRINCIPLES" (see page 320), which includes general information on "Firewall Characteristics" (see page 321) and "Types of Firewalls" (see page 322). Moreover, Fig. 10.1(a) from Stallings merely illustrates a "Packet-filtering router" between the "Internet" and the "Private network."

However, disclosing that a user may connect to a remote computer utilizing a communications program (see Reinert), utilizing a VPN or a SSL to create a secure connection (see Yadav), along with a general firewall description (see Stallings), fails to specifically teach that "network support code is used to enable said computer to establish said secure network connection via said firewall computer to said remote computer" (emphasis added), as claimed by appellant. Appellant respectfully asserts that only appellant teaches and claims the loading of network support code from removable physical media which specifically enables the secure network connection via the firewall, in the context claimed.

In addition, the Examiner has specifically argued that "[i]n light of [appellant's previous] amendments, the Stallings reference is submitted," and that "[a]s herein modified, the code [of Reinert] is also used to establish the secure connection via said firewall, as the packets must traverse the firewall for reception at the remote computer" (see page 5 of the Office Action dated 05/15/2007). Appellant respectfully disagrees and asserts that even in view of the improper combination of the Reinert, Yadav, and Stallings references, the proposed combination fails to teach or suggest that "said network support code is used to **enable** said computer to establish said secure network connection **via said firewall** computer to said remote computer" (emphasis added), in the context claimed by appellant, for at least the reasons noted above.

Appellant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, since it would be *unobvious* to combine the references, as noted above, and the prior art excerpts, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above.

Group #2: Claim 29

With respect to Claim 29, the Examiner has relied on Col. 8, lines 14-16 and lines 25-31 from the Reinert reference to make a prior art showing of appellant's claimed technique "wherein said one or more malware detection files are determined based on said non-installed operating system."

Appellant respectfully asserts that the excerpts from Reinert relied upon by the Examiner merely teach that "a service program is downloaded from the remote computer 54 to the local computer 42" (Col. 8, lines 14-16 - emphasis added), and that "[d]ownloading the virus scanning software into the local computer memory 41 provides advantages ... because the virus scanning and virus repairing programs may be executed in the local computer memory" (Col.8, lines 25-29 – emphasis added). However, simply disclosing that a program is downloaded from the remote computer to the local computer and may be executed in local memory, as in Reinert, fails to even suggest that "one or more malware detection files are determined based on said non-installed operating system" (emphasis added), as specifically claimed by appellant.

Appellant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, since it would be *unobvious* to combine the references, as noted above, and the prior art excerpts, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above.

Group #3: Claim 30

With respect to Claim 30, the Examiner has relied on Col. 8, lines 20-35 from the Reinert reference to make a prior art showing of appellant's claimed technique "wherein said one or more malware detection files are determined based on a malware detection product." Specifically, the Examiner has argued that "the virus detection signature file is used by the virus scanning software utility program."

Appellant respectfully disagrees and asserts that the excerpt relied upon by the Examiner merely teaches that "[i]f the local computer 42 requests virus scanning services, a virus scanning software utility program is downloaded into the local computer memory 41 via communications

hardware modems 58 and 40, respectively," and that "a complete up-to-date virus signature file is downloaded into the local computer memory 41" (Col. 8, lines 20-25).

However, downloading a virus scanning software utility program as well as a virus signature file, as in Reinert, fails to specifically suggest a technique "wherein said one or more malware detection files are determined based on a malware detection product" (emphasis added), as claimed by appellant. Moreover, asserting that "the virus detection signature file is used by the virus scanning software utility program," as argued by the Examiner, fails to suggest that "one or more malware detection files are determined based on a malware detection product" (emphasis added), as claimed by appellant.

Appellant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, since it would be *unobvious* to combine the references, as noted above, and the prior art excerpts, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above.

Issue #2:

The Examiner has rejected Claims 26-27 under 35 U.S.C. 103(a) as being unpatentable over Reinert (U.S. Patent No. 6,347,375) in view of Yadav (U.S. Publication No. 2003/0149887), in view of Stallings ("Network Security Essentials, Applications and Standards), and in further view of Khatri (U.S. Patent No. 6,721,883).

Group #1: Claim 26

Appellant respectfully asserts that such claims are not met by the prior art for the reasons argued with respect to Issue #1, Group #1.

Group #2: Claim 27

Appellant respectfully asserts that such claims are not met by the prior art for the reasons argued with respect to Issue #1, Group #1.

Issue #3:

The Examiner has rejected Claim 31 under 35 U.S.C. 103(a) as being unpatentable over Reinert (U.S. Patent No. 6,347,375) in view of Yadav (U.S. Publication No. 2003/0149887), in view of Stallings ("Network Security Essentials, Applications and Standards"), and in further view of McCoskey (U.S. Publication No. 2003/0028889).

Group #1: Claim 31

Appellant respectfully asserts that such claims are not met by the prior art for the reasons argued with respect to Issue #1, Group #1.

Issue #4:

The Examiner has not specifically rejected Claims 5, 9, 13, 17, 21, 25, and 31 under 35 U.S.C. 112. However, in the Office Action dated 05/15/2007, the Examiner has responded to appellant's arguments from the Amendment dated 03/12/2007 regarding the 35 U.S.C. 112 rejection from the Office Action dated 12/11/2006.

Group #1: Claims 5, 9, 13, 17, 21, and 25

Specifically, with respect to Claims 5, 9, 13, 17, 21, and 25, the Examiner has argued that "[t]he limitation recited that a firewall is disposed between the computer being controlled by the removable physical media and the remote computer appears to have no limiting effect on the removable physical media itself."

Appellant respectfully disagrees and asserts that appellant specifically claims a technique "wherein a firewall computer disposed between said computer and said remote computer is operable to block a connection between said computer and said remote computer other than said secure network connection," and that "said network support code is used to enable said computer to establish said secure network connection via said firewall computer to said remote computer,"

in the context claimed (see this or similar, but not necessarily identical language in the aforementioned independent claims - emphasis added). Thus, appellant's "firewall...," as claimed, does indeed add to the limitations of the claims as "said network support code is used to enable said computer to establish said secure network connection via said firewall computer to said remote computer" (emphasis added), in the context claimed by appellant.

Still yet, with respect to Claim 25, the Examiner has argued that "[certain] limitations are in question because the claim is directed to a server computer and the...limitations appear to provide no further components of the server computer." Appellant respectfully disagrees and asserts that, with respect to the claim limitations in question, appellant claims that the "computer is booted with a non-installed operating system ... [and that the] network support code is loaded for said computer ... [and] malware detection is performed upon said computer" (emphasis added), and that therefore such limitations do add to the server computer because "[the] server computer [is] connected by a network link to [the] computer" (emphasis added), in the context claimed by appellant. Additionally, with respect to the claim limitations in question, appellant clearly claims that "network support code is used to enable said computer to establish said secure network connection via said firewall to said server computer" (emphasis added), and that "malware detection is performed upon said computer using said one or more malware detection files," where the server "load[s] [the] one or more malware detection files to said computer," in the context claimed.

Group #2: Claim 31

Further, with respect to Claim 31, the Examiner has argued that 'the limitation "wherein said remote computer logs said downloading of said one or more malware detection files by said computer" appears to have no effect on the claim because claim 1 is directed to a removable physical media which does not necessarily change as a result of the actions of a remote computer.' Appellant respectfully disagrees and asserts that appellant clearly claims "log[ging] said downloading of said one or more malware detection files by said computer," where "one or more malware detection files [are downloaded from the remote computer]," in the context claimed.

In view of the remarks set forth hereinabove, all of the independent claims are deemed allowable, along with any claims depending therefrom.

VIII CLAIMS APPENDIX (37 C.F.R. § 41.37(c)(1)(viii))

The text of the claims involved in the appeal (along with associated status information) is set forth below:

1. (Previously Presented) A removable physical media bearing a computer program operable to control a computer to detect malware by performing the steps of:

booting said computer with a non-installed operating system read from said removable physical media instead of an installed operating system stored on said computer;

loading network support code for said computer read from said removable physical media;

downloading from a remote computer one or more malware detection files;

performing malware detection upon said computer using said one or more malware detection files; and

establishing a secure network connection to said remote computer;

wherein a firewall computer disposed between said computer and said remote computer is operable to block a connection between said computer and said remote computer other than said secure network connection;

wherein said network support code is used to enable said computer to establish said secure network connection via said firewall computer to said remote computer.

2. (Original) A removable physical media as claimed in claim 1, wherein said one or more malware detection files include at least one of:

malware definition data containing data characteristic of malware to be detected;

a malware detecting engine operable to control said computer to perform said malware detection;

a malware application shell; and

malware detection option settings operable to configure optional settings of said malware detection.

3. (Original) A removable physical media as claimed in claim 1, wherein said steps further comprise loading security management code operable to control said downloading.

4. (Cancelled)

5. (Cancelled)

6. (Cancelled)

7. (Original) A removable physical media as claimed in claim 1, wherein said removable physical media is one of:

an optical disk;

a floppy disk;

a memory card; and

a removable disk drive.

8. (Original) A removable physical media as claimed in claim 1, wherein malware to be detected includes one or more of:

a computer virus;

a computer Trojan;

a computer worm;

a banned computer application;

a data file associated with a malware file; and

configuration settings of said computer associated with a malware file.

9. (Previously Presented) A method of detecting malware upon a computer, said method comprising:

booting said computer with a non-installed operating system read from a removable physical media instead of an installed operating system stored on said computer;

loading network support code for said computer read from said removable physical media;

downloading from a remote computer one or more malware detection files;

performing malware detection upon said computer using said one or more malware detection files; and

establishing a secure network connection to said remote computer;

wherein a firewall disposed between said computer and said remote computer is operable to block a connection between said computer and said remote computer other than said secure network connection;

wherein said network support code is used to enable said computer to establish said secure network connection via said firewall to said remote computer.

10. (Original) A method as claimed in claim 9, wherein said one or more malware detection files include at least one of:

malware definition data containing data characteristic of malware to be detected;

a malware detecting engine operable to control said computer to perform said malware detection;

a malware application shell; and

malware detection option settings operable to configure optional settings of said malware detection.

11. (Original) A method as claimed in claim 9, comprising loading security management code operable to control said downloading.

12. (Cancelled)

13. (Cancelled)

14. (Cancelled)

15. (Original) A method as claimed in claim 9, wherein said removable physical media is one of:

an optical disk;

a floppy disk;

a memory card; and

a removable disk drive.

16. (Original) A method as claimed in claim 9, wherein malware to be detected includes one or more of:

a computer virus;

a computer Trojan;

a computer worm;

a banned computer application;

a data file associated with a malware file; and

configuration settings of said computer associated with a malware file.

17. (Previously Presented) A computer operable to detect malware upon said computer, said computer comprising a processor configured to perform the steps of:

booting said computer with a non-installed operating system read from a removable physical media instead of an installed operating system stored on said computer;

loading network support code for said computer read from said removable physical media;

downloading from a remote computer one or more malware detection files;

performing malware detection upon said computer using said one or more malware detection files; and

establishing a secure network connection to said remote computer;

wherein a firewall computer disposed between said computer and said remote computer is operable to block a connection between said computer and said remote computer other than said secure network connection;

wherein said network support code is used to enable said computer to establish said secure network connection via said firewall computer to said remote computer.

18. (Original) A computer as claimed in claim 17, wherein said one or more malware detection files include at least one of:

malware definition data containing data characteristic of malware to be detected;

a malware detecting engine operable to control said computer to perform said malware detection;

a malware application shell; and

malware detection option settings operable to configure optional settings of said malware detection.

19. (Original) A computer as claimed in claim 17, wherein said steps further comprise loading security management code operable to control said downloading.

20. (Cancelled)

21. (Cancelled)

22. (Cancelled)

23. (Original) A computer as claimed in claim 17, wherein said removable physical media is one of:

an optical disk;

a floppy disk;

a memory card; and

a removable disk drive.

24. (Original) A computer as claimed in claim 17, wherein malware to be detected includes one or more of:

a computer virus;

a computer Trojan;

a computer worm;

a banned computer application;

a data file associated with a malware file; and

configuration settings of said computer associated with a malware file.

25. (Previously Presented) A server computer connected by a network link to a computer detecting malware upon said computer, said server computer comprising a processor configured to perform the steps of:

establishing a secure network connection to said computer; and

loading one or more malware detection files to said computer;

wherein a firewall disposed between said computer and said server computer is operable to block a connection between said computer and said server computer other than said secure network connection;

wherein said computer is booted with a non-installed operating system read from a removable physical media instead of an installed operating system stored on said computer;

wherein network support code is loaded for said computer read from said removable physical media;

wherein said network support code is used to enable said computer to establish said secure network connection via said firewall to said server computer;

wherein malware detection is performed upon said computer using said one or more malware detection files.

26. (Previously Presented) A removable physical media as claimed in claim 1, wherein said computer is configured in its BIOS settings to boot from said removable physical media.

27. (Previously Presented) A removable physical media as claimed in claim 1, wherein booting said computer with said non-installed operating system read from said removable physical media is based on a determination that a bootable removable media is present.

28. (Previously Presented) A removable physical media as claimed in claim 1, wherein said remote computer determines said one or more malware detection files that are downloaded to said computer.

29. (Previously Presented) A removable physical media as claimed in claim 28, wherein said one or more malware detection files are determined based on said non-installed operating system.

30. (Previously Presented) A removable physical media as claimed in claim 28, wherein said one or more malware detection files are determined based on a malware detection product.

31. (Previously Presented) A removable physical media as claimed in claim 1, wherein said remote computer logs said downloading of said one or more malware detection files by said computer.

IX EVIDENCE APPENDIX (37 C.F.R. § 41.37(c)(1)(ix))

There is no such evidence.

X RELATED PROCEEDING APPENDIX (37 C.F.R. § 41.37(c)(1)(x))

N/A

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 971-2573. For payment of any additional fees due in connection with the filing of this paper, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1351 (Order No. NAI1P492).

Respectfully submitted,

By: /KEVINZILKA/ Date: December 13, 2007
Kevin J. Zilka
Reg. No. 41,429

Zilka-Kotab, P.C.
P.O. Box 721120
San Jose, California 95172-1120
Telephone: (408) 971-2573
Facsimile: (408) 971-4660